Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

DETERMINATION OF ALL GROUPS OF BINARY LINEAR SUBSTITUTIONS WITH INTEGRAL COEFFICIENTS TAKEN MODULO 3 AND OF DETERMINANT UNITY

BY LEONARD EUGENE DICKSON

1. Introduction. This elementary example is chosen by way of illustration of the methods of linear group theory and in view of applications the results have in an investigation now in progress.

Let p be a prime number and consider the $p^2 - 1$ letters $l_{x,y}$, where x and y take independently the values $0, 1, \ldots, p-1$, such that x and y are not both 0. If $\alpha, \beta, \gamma, \delta$ are any integers such that $\alpha\delta - \beta\gamma \equiv 1 \pmod{p}$, the operation which replaces $l_{x,y}$ by $l_{x',y'}$, where

$$(1) \qquad x' \equiv \alpha x + \beta y, \quad y' \equiv \gamma x + \delta y \pmod{p},$$

defines a substitution $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ on the $p^2 - 1$ letters $l_{x,y}$. The totality of these substitutions constitutes a group Γ of order $p(p^2-1)$.

For $p = 2$, Γ is the symmetric group on the 3 letters $l_{1,0}$, $l_{0,1}$, $l_{1,1}$.

For $p = 3$, Γ is of order 24. Its degree, the number of the letters $l_{x\,y}$, is 8. It is shown in §5 that Γ cannot be represented as a substitution-group of degree less than 8.

The object of this note is to give an elementary determination of all the subgroups of Γ_{24} and to make a distribution of its substitutions into complete sets of conjugates. As indicated in §6, the first problem can be solved for any p by employing technical group theory and making use of the results of elaborate memoirs on the modular group.

2. Periods of the substitutions of Γ_{24}. Observing that, if $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$,

$$(2) \qquad S^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}, \quad S^2 = \begin{pmatrix} \alpha^2 + \beta\gamma & \beta(\alpha+\delta) \\ \gamma(\alpha+\delta) & \delta^2 + \beta\gamma \end{pmatrix},$$

we find that the only substitution of period 2 is $E = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and that, if S

be neither E nor the identity I, S is of period 3 if and only if $\alpha + \delta \equiv -1$, of period 4 if and only if $\alpha + \delta \equiv 0$, of period 6 if and only if $\alpha + \delta \equiv +1$ (mod 3). Hence Γ_{24} contains, in addition to E and I, exactly

8 substitutions of period 3 : $\begin{pmatrix} 0 & \pm 1 \\ \mp 1 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ \pm 1 & 1 \end{pmatrix}$, $\begin{pmatrix} -1 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}$;

6 substitutions of period 4 : $\begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & \pm 1 \\ \pm 1 & -1 \end{pmatrix}$, $\begin{pmatrix} -1 & \pm 1 \\ \pm 1 & 1 \end{pmatrix}$;

8 substitutions of period 6 : $\begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 1 \end{pmatrix}$, $\begin{pmatrix} -1 & \pm 1 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} -1 & 0 \\ \pm 1 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}$.

3. Distribution into sets of conjugate substitutions.

If $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, then

$$S^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}S = \begin{pmatrix} 1 - \alpha\gamma & \alpha^2 \\ -\gamma^2 & 1 + \alpha\gamma \end{pmatrix} \equiv S_1, \tag{3}$$

$$S^{-1}\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}S = \begin{pmatrix} -\alpha\gamma - \beta\gamma - \beta\delta & (\alpha - \beta)^2 \\ -(\gamma - \delta)^2 & \alpha\gamma + \alpha\delta + \beta\delta \end{pmatrix} \equiv S_2.$$

Since -1 is a quadratic non-residue of 3, S_1 reduces to none of the substitutions

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & -1 \\ +1 & 0 \end{pmatrix}, \tag{4}$$

each of period 3. Again, S_1 reduces to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ if and only if $\gamma \equiv 0$, $\alpha \equiv \delta \equiv \pm 1$, β remaining arbitrary (mod 3). Since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is therefore commutative with exactly 6 substitutions of Γ_{24}, it is conjugate with exactly four substitutions. From what precedes, these must be*

$$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}. \tag{5}$$

Their inverses are respectively the substitutions (4). Hence the latter are conjugate.

---

* This may be verified directly. Thus $S_1 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ if and only if $\alpha \equiv \gamma = \pm 1$, $\delta \equiv \beta \pm 1$.

Likewise, S_2 reduces to none of the substitutions, each of period 6:

$$(6) \qquad \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ +1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}.$$

Again, S_2 reduces to $\begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}$ if and only if $\alpha \equiv \beta = \pm 1$, $\delta \equiv \gamma \pm 1$; S_2 reduces to $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ if and only if $\delta \equiv \alpha$, $\beta \equiv \alpha \pm 1$, $\gamma \equiv \alpha \mp 1$; S_2 reduces to $\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ if and only if $\gamma \equiv \delta = \pm 1$, $\alpha \equiv \beta \pm 1$. Hence a complete set of conjugates is given by

$$(7) \qquad \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.$$

Their inverses are respectively the substitutions (6). Hence the latter are conjugate.

Finally, $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is commutative with $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ if and only if $\alpha \equiv \delta$, $\beta \equiv -\gamma$. Since S shall have determinant $+1$, $\alpha^2 + \gamma^2 \equiv 1$, so that either $\alpha \equiv 0$, $\gamma \equiv \pm 1$ or else $\alpha \equiv \pm 1$, $\gamma \equiv 0$. The resulting 4 substitutions S are evidently the powers of $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Hence the latter is one of 4 conjugates.

THEOREM. *Within* Γ_{24}, *the substitutions of period* 3 *fall into the two distinct sets of conjugates* (4) *and* (5); *the substitutions of period* 6 *fall into the two distinct sets of conjugates* (6) *and* (7); *the substitutions of period* 4 *are all conjugate.*

4. Determination of all the subgroups of Γ_{24}. It follows from §3 that Γ_{24} has exactly 4 subgroups of order 3 and that they are all conjugate. The latter result also follows from Sylow's theorem. Likewise, by §3, Γ_{24} has exactly 4 cyclic subgroups of order 6, all conjugate within Γ_{24}, and exactly 3 cyclic subgroups of order 4, all conjugate. By §2, Γ_{24} contains a single (and hence self-conjugate) subgroup of order 2.

Since any substitution of period 4 is conjugate with its inverse by §3, any cyclic subgroup of order 4 is self-conjugate under exactly a dihedron subgroup of order 8. In view of the enumeration of the substitutions of Γ_{24}, the latter has a single (and hence self-conjugate) subgroup of order 8, composed of I, E, and the 6 substitutions of period 4.

A subgroup of order 6 containing a single operator of period 2 is cyclic.

Finally, there is no subgroup of order 12. For, by Sylow's theorem, a G_{12} contains 1 or 3 conjugate G_4 and 1 or 4 conjugate G_3. Within Γ_{24}, any G_4 is self-conjugate only under a G_8, while any G_3 is self-conjugate only under a G_6, as shown above. Hence G_{12} contains 3 conjugate G_4 and 4 conjugate G_3, and therefore at least $3 \times 2 + 4 \times 2$ or 14 substitutions in addition to I and E. Hence G_{12} cannot exist.

THEOREM. *The group Γ_{24} contains one self-conjugate cyclic C_2 and one self-conjugate dihedron G_8, one set of 3 conjugate cyclic C_4, one set of 4 conjugate cyclic C_3, one set of 4 conjugate cyclic C_6, but no further subgroups other than itself and the identity.*

5. Isomorphism of Γ_{24} with known groups. Since Γ_{24} has no subgroup of order 12 it is generated by any one of its operators of period 3 together with any one of its operators of period 4. Now $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ give rise to the following substitutions on the letters $l_{x,y}$:

$$(l_{1,2}l_{0,2}l_{2,2})(l_{2,1}l_{0,1}l_{1,1}), \quad (l_{1,2}l_{1,1}l_{2,1}l_{2,2})(l_{0,1}l_{2,0}l_{0,2}l_{1,0}),$$

respectively. Hence Γ_{24} may be immediately identified with the group No. 10 under those of order 24 and degree 8 in Miller's list (*American Journal of Mathematics*, vol. 21, p. 332), and, as there indicated, is not simply isomorphic with a substitution-group of degree less than 8.

In Burnside's enumeration (*Theory of Groups*, pp. 101–104) of the 15 distinct types of abstract groups of order 24, our group Γ_{24} falls under type (IV), case 1. Hence it is simply isomorphic with the abstract group generated by three operators A, B, C, subject to the generational relations

$$(8)\quad A^4 = I,\ B^2 = A^2,\ B^{-1}AB = A^{-1},\ C^3 = I,\ C^{-1}AC = B,\ C^{-1}BC = AB.$$

6. Indirect method of determining the subgroups of Γ. The group Γ of the linear substitutions (1) of determinant unity is isomorphic (simply if $p = 2$, doubly if $p > 2$) with the group F of the modular substitutions

$$(9)\qquad z' = \frac{\alpha z + \beta}{\gamma z + \delta} \qquad (\alpha\delta - \beta\gamma = 1).$$

In fact, I and E, but no further substitutions (1), correspond to the identity modular substitution $z' = z$. Hence the quotient-group $\Gamma/(I, E)$ is simply isomorphic with F From the known* subgroups of F we may derive indirectly the subgroups of Γ; the inverse problem is more easily solved. A direct generalization is obtained by replacing the field of integers modulo p by the Galois field of order p^n; the subgroups of the resulting group F are known.†

Consider, for example, the case $p^n = 3$. The group F of the substitutions (9) is then simply isomorphic with the alternating group on 4 letters and hence has, in addition to itself and identity, only subgroups of the type cyclic C'_2, cyclic C'_3, and the commutative "four-group" K_4. We may thus derive the theorem of §4. Thus $I \sim C_2$, $C'_2 \sim C_4$, $C'_3 \sim C_3$ or C_6, $K_4 \sim G_8$, $F \sim \Gamma_{24}$.

The University of Chicago,
July, 1903.

---

*Gierster, *Mathematische Annalen*, vol. 18 (1881); Klein-Fricke, *Modulfunctionen*, I, p. 411 and pp. 419-491.

† Moore, The subgroups of the Generalized Finite Modular Group, *University of Chicago Decennial Publications*, vol. 9 (1903), abstract in *Bulletin Amer. Math. Soc.*, vol. 5 (1898), pp. 7-8; Wiman, *Swedish Acad.*, vol. 25 (1899), pp. 1-47; Dickson, *Linear Groups*, pp. 260-287.